REMARKS

Claims 1-3, 6, 9-14, 17-21, 23-58 are pending. Claims 1, 3, 9, 10, 12, 13, 14, 19-21, 23-25, 27-29, 32, 37, 40-47, 50-52 and 57 have been amended. Claims 4-5, 7-8, 15-16, 22 were canceled. New claim 58 has been added.

In response to the examiner's section 112 rejections, claims 1, 10, 12, 13, 14, 21, 24, 27, 29, 32, 40-47, 50-51 and 57 have been amended to make these claims clear and definite. In the case of domain filtering in claims 1 and 57, the amendments define the domain filtering engine to be capable of using the inbound lists or using both inbound an outbound lists. Claims 37 and 52 have been amended to correct a lack of antecedent basis for "first proxy server".

In response to the examiner's prior art rejections, Applicant has amended independent claims 1, 14 and 57.

For example claims 1 and 57 have been amended with regard to domain filtering to recite, "the "requesting client" is at least one (i) an HTTP (Hypertext Transfer Protocol) client and (ii) a web browser". The HTTP client is often the browser although it does not have to be. This amendment is supported in the original disclosure including FIG. 8A, FIG. 8B, page 15 of the Specification at lines 2-3, 7, 11 mentioning "HTTP client". Furthermore, the patent application states that it incorporates by reference in its entirety parent application 09/661,876 which has since matured into U.S. Patent No. 7,587,499 B1. Support for the amendment appears in this parent application at column 3 lines 22-23, 45-49 and in column 4 lines 22 and 49.

A note about the form used in certain claims. It should be understood that the term <u>"requesting clients"</u> (the underlining used here to make it clear that the

quotes are included in the referred-to term) is a more aesthetically appealing way of writing "requesting client"s. Although only the singular version ("requesting client") appears in independent claim 1 with the quotes, dependent claims 10 and 50 put quotes around the plural version. Therefore, Applicant wishes to make sure that there is no confusion and that it is clear that the plural version is not a new entity but rather merely the plural of the single entity that was in quotes.

This amendment distinguishes the claimed invention over the cited prior art. It was previously argued in the last amendment that the prior art, such as Gatz, does not teach client application authentication. The examiner countered in item 7 on page 3 of the Office Action that Applicant did not claim this. With the amendments herein to claims 1 and 57, Applicant is now explicitly claiming client application authentication. Column 3 lines 27-30 defines "HTTP clients" as "HTTP applications..." Gatz does not teach client application authentication. See Gatz para. 0061 and FIG. 6 items 84, 85. Gatz design does not support client application authentication and is inconsistent regarding the type of clients. For example, Gatz calls user computers "clients" 212(1) through 212(N). See Gatz "user computer" 212(1) thru 212(N) in Figure 2, and [0045], particularly, lines 1-3 but he calls his 212 a "user." See Gatz [0044]. He calls a client as: "Client Computer Devices 8, 10 ...". See [0042], as well as Figure 1. He further, calls a client as: "HTTP client 212..." See [0045], and Figure 2. Gatz also discloses: "... user computer system or device 212 to have basic hardware ... having display screen... " - as seen in Figure 2 -. See Gatz [0050]. Gatz also discloses device 212 to have input devices as well as output devices. See Gatz [0051], and [0052].

Moreover, Humes does not teach client application authentication since its checks

based on the identity of the URL and not based on the identity of applications. Furthermore, Cirasole does not teach client application authentication since it uses the term "client" to refer to computers. For example in Cirasole at column 3 lines 59-64 it states "The clients, 11, 12, and 13 as shown, may be using any of a number of platforms such as the Windows™, MacOS™, or Unix™ operating systems". So the clients are computers, not applications.

It has been noted previously that client application identity authentication is extremely important since often multiple applications share the same client host identities. The use of client application identity includes vendors' information, version, client host information, and even hardware information. The client application information will be used for many reasons, such as: a) session information – for security reasons-; b) for client host IP address and domain name; c) to resolve the type of client application (i.e., which browser type) in order to allow the responding server to provide appropriate responses for Presentation Support, and d) etc. There are more than a dozen browsers available in the smart phone market; each supports a different presentation format. The server has to know the type and version of the browser to properly send the response. This improves the authentication process.

As an example of the above, performing client application authentication, such as an HTTP browser will be important for preventing some session hijacking attacks since any responding resource server can differentiate two client applications on a single host machine. In contrast, relying on client host authentication as taught in the prior art creates a window of opportunity for impersonating rouge applications - that have successfully hijacked the legitimate application sessions and user sessions. Rouge

applications such as Trojan horse can run on the host computer and wait for a user to authenticate to web sites with high value resources – using a HTTP client application such as a browser. Upon a successful authentication, they will use the hijacked session information for independent operation behind the scene. Since both rouge and legitimate applications have identical host machine information, a serious security breach can occur without client application authentication of the claimed invention. A client application authentication can significantly help the server to reject requests from a rouge application. Client application authentication can also be used against Cyber threats such as Cross Site Request Forgery XSRF attacks.

While the use of client host identity is a subset of client application identity, the reverse is not correct. That means that while a client host IP address is available to the client application, the client application identity is not available to the client host. Therefore, such client host identity information can be extracted from a client application identity as an additional piece of information. Note that IP address is one example of client application identity, although not the only possible example.

It is respectfully submitted that independent claims 1 and 57 are novel and nonobvious over the prior art and should be allowed along with their dependent claims 2-3, 6, 9-13, 17-54, 58.

Applicant has also amended independent claim 14, which involves content filtering, to recite checking the content of the requested document "during a web server response to a request for a web resource". The amendment makes clear that the checking of the requested document against the friendly or unfriendly inbound list is occurring "during a web server response to a request for a web resource". Applicant has also

amended claim 14 to recite "the security and filtering software configured to perform the content filtering including the checking independent of whether the security and filtering software has performed domain filtering". This distinguishes it from Humes, see column 3 lines 23-40, FIGS. 2-3, where the content filtering (i.e. checking the words of a web site) occurs after checking the URL. For example, in Humes FIG. 3, the content filtering only occurs after the URL is checked to see if the URL is in the Deny or Allow list. Accordingly, the Humes software is not configured to perform the content filtering independent of whether the software has performed domain filtering, as it is in the claimed invention.

The amendment to claim 14 referred to is supported at least in FIG. 2, which clearly shows that the request document is filtered for content during the server's response to the client request. In addition, the amendment is supported at column 3 lines 50-54 of the parent application referred to above, which states that the web server serves the clients "by responding to requests from the "clients" for resources (the web site)". Furthermore, the amendment to claim 14 reciting "the software configured to perform the content filtering, including the checking, independent of whether the software has performed domain filtering" is supported at FIGS. 5A, 5B, 5C, 6A, 6B, 6C, 6D and the discussion of these figures. These figures clearly show content filtering occurring independent of any domain filtering. Although domain filtering may still occur in the software 10 of the claimed invention, the content filtering engine is configured to perform the content filtering independently of the domain filtering engine, unlike in Humes. Furthermore, the other cited art do not teach this claim limitation or do not even teach content filtering.

Since neither Humes nor the other prior art meet this claim limitation, claim 14 is distinguishable over the prior art. Consequently, dependent claims 17, 46-54 are also distinguishable over the prior art.

Regarding claim 9, Applicant has amended this claim to recite that the "portion" is less than the entire e-mail message, although any other interpretation is not really consistent with English. This amendment distinguishes over Gennaro and the other prior art. Gennaro does not teach that the user can select what portion of the e-mail message to encrypt and the encryption function can then encrypt only that portion. This provides an advantage over data mining programs without having to encrypt the entire message.

New claim 58 tracks the last part of claim 57, as amended, except that new claim 58 is dependent on claim 10.

The claimed invention of claims 1 and 57 also have numerous other differences and advantages over the prior art. For example, Gatz deals with corporate resource protection and not web access management. The Gatz system is not scalable or reliable, utilizes multiple administrative domains and would be insecure for its users since it would not protect against impersonation. Gatz also does not support content filtering or the claims limitations of the present invention related to content filtering. Humes' content filtering is not scalable, or definite.

An amendment to page 5 of the Specification has been made herein to clarify that the objects and advantages may be present in certain embodiments.

In response to the examiner's double patenting rejection of claim 1, Applicant previously filed a corrected terminal disclaimer with respect to US Patent No. 7,587,499 (the parent) on December 19, 2011, which appears on Public Pair.

It is respectfully requested that claims 1-3, 6, 9-14, 17-21, 23-58, which are understood to be in condition for allowance, be allowed.

Dated: March 29, 2012

Respectfully submitted,

Mark M. Friedman
Attorney for Applicant
Registration No. 33,883
Dr. Mark Friedman Ltd.
Moshe Aviv Tower, 54th Floor
7 Jabotinsky Street
Ramat Gan 52520 ISRAEL
Tel: 972-3-6114100
Fax: 972-3-6114101
Email: patents@friedpat.com